**KAPLAN FOX & KILSHEIMER LLP**
Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
Email: *lking@kaplanfox.com*
*mgeorge@kaplanfox.com*
*breed@kaplanfox.com*

**KANTROWITZ, GOLDHAMER & GRAIFMANAN, P.C.**
Melissa R. Emert (admitted *pro hac vice*)
Gary S. Graifman (admitted *pro hac vice*)
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Facsimile: 302-307-1086
Email: *memert@kgglaw.com*
*ggraifman@kgglaw.com*

*Interim Co-Lead Class Counsel*

*Attorneys for Plaintiffs*

[*Additional Counsel Appear on Signature Page*]

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

| | |
|---|---|
| *In re: Illuminate Education Data Security Incident Litigation* | Case No. 8:22-cv-1164-JVS-ADSx<br><br>**REDACTED VERSION OF CONSOLIDATED AMENDED CLASS ACTION COMPLAINT**<br><br>**FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED JUNE 21, 2023**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiffs Lucas Cranor, Kristen Weiland, Anastasiya Kisil, Tara Chambers, Janene Vitro and Lorraine Deniz ("Plaintiffs"), by and through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant Illuminate Education, Inc. ("Illuminate" or "Defendant") and make the following allegations based upon personal knowledge as to themselves and their own acts, and upon information and belief based on the investigation of counsel, as to all other matters, as follows:

## INTRODUCTION

1. This is not a run-of-the mill data breach case. This is a case involving a data breach [redacted] on Illuminate, a company that is in the for-profit business of storing minors' immutable information such as economic status, birth dates, academic status, learning disability information, and other behavioral and health information. Where a cyberattack exposes this kind of information to criminal third-parties, and, where, as explained below, the company entrusted with such information failed to encrypt and safeguard that information, that company is liable under applicable legal precedent.

2. Illuminate is a software company focused on education that provides "a streamlined solution that helps educators to accurately assess learning, identify needs, align whole child supports, and drive school improvement in order to equitably accelerate growth for every learner."[1]

3. In 2019, Illuminate acquired another educational technology company, FastBridge Learning, and by January 2020, Illuminate was servicing 17 million students in 5,200 schools and districts across all 50 states.

4. Illuminate has several products currently at use in America's schools that require the collection of students' personal information, including but not limited to the following Illuminate platforms:

[1] *See* https://www.illuminateed.com (last visited May 30, 2023).

- FastBridge, which can identify "students' academic and social-emotional behavior (SEB) needs faster, align the right interventions at the right time, and measure whether interventions are helping students catch up…"[2];
- Data and Assessment ("DnA"), a standards-based assessment creation administration solution…"[3]; and
- eduCLIMBER, an "[I]nteractive district-level to whole-child data management that strengthens MTSS implementations, including student need identification and intervention effectiveness."[4]

5. Illuminate also offers popular platforms for districts and schools, such as Skedula, IO Classroom, and PupilPath.

6. These products collect, among other things, students' attendance and grades, names, birth dates, class schedules, behavioral records, and health and socio-economic information such as whether they qualify for special education or free or reduced-price lunches.[5] As part of its core business in providing education-related software, Illuminate also stores demographic information, including student names, mailing and email addresses, dates of birth, student education and behavioral records, health-related information, including student immunizations, and vision and hearing screening results, and system usernames and passwords.[6] Thus, the information the products collect is private, sensitive and immutable.

---

[2] *See* https://www.illuminateed.com/products/fastbridge/ (last visited May 31, 2023).

[3] *See* https://www.illuminateed.com/products/dna/?utm_source=Website%3A+Main+Homepage&utm_medium=Website&utm_content=Learn+More+About+DnA&utm_campaign=2020+Website+Updates (last visited May 31, 2023).

[4] *See* https://www.illuminateed.com/products/educlimber/?utm_source=Website%3A+Main+Homepage&utm_medium=Website&utm_content=Learn+More+About+eduCLIMBER&utm_campaign=2020+Website+Updates (last visited May 31, 2023).

[5] *See* https://www.the74million.org/article/74-interview-cybersecurity-expert-levin-on-the-harms-of-student-data-hacks/ (last visited May 31, 2023).

[6] *See* https://www.illuminateed.com/resources/security-privacy/ (last visited May 31, 2023).

7. Because of the largely sensitive and immutable information Illuminate was entrusted with and promised to protect, it had a duty to employ reasonable safety protections and procedures normally employed by similar companies in the industry. Illuminate also had a duty to protect this information from third parties under various statutes. As detailed below, Illuminate, because of its inadequate and lax security measures, breached these duties, resulting in Plaintiffs' and class members' sensitive information falling into the hands of cybercriminals.

8. Indeed, on or about January 8, 2022 Illuminate learned that the databases on which it maintained the personally identifiable information ("PII") and other data for millions of students had been compromised by cybercriminals. [redacted]. However, this information was not disclosed to Plaintiffs and class members and Illuminate did not disclose the Data Breach to Plaintiffs and class members until at least three months after the Data Breach took place.

9. [redacted]

10. [redacted]. Yet, it was not until approximately April 2022 that Illuminate started to inform students and their parents about the data breach, and, even then, downplayed the seriousness of

the situation by merely telling them that certain of Illuminate's databases containing their information were subject to "unauthorized access" between December 28, 2021 and January 8, 2022. [redacted].[8] By keeping this information from the millions of victims of this data breach, Illuminate has deprived the victims of vital information about the situation and, accordingly, many may not take steps to adequately protect themselves from identity theft and other harms.

11. Additionally, as has been learned through discovery conducted to date, contrary to its obligations under various statutes, contracts with various school systems and expected practice of a company that gathers and maintains the type of sensitive personal information of minor students, Illuminate failed to encrypt such data and further, did not have in place appropriate and expected protocols concerning the ability to access the data that was subject to this data breach. The result being what happened here – one of the worst, if not the worst, data breaches ever committed concerning sensitive student data, which will put millions at risk for years to come.

12. Plaintiffs bring this class action alleging that Defendant's conduct, as described more fully herein, caused Plaintiffs' and Class Members' Private Information to be exposed and stolen because of the failure of Defendant to safeguard and protect their sensitive information. Plaintiffs seek damages, and injunctive and other relief, on behalf of themselves and similarly situated consumers.

## PARTIES

13. Plaintiff Cranor is a resident of Colorado. Mr. Cranor received two notice letters from Illuminate dated April 29, 2022, stating that both of his children's

[7]

[8] [redacted]

Private Information was compromised by the Data Breach. Mr. Cranor's children are minors who attend school in Colorado. Plaintiff is filing these claims as a real party in interest for himself and his minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

14. Plaintiff Weiland is a resident of Colorado. Ms. Weiland received one or more notice letters from the Douglas County, Colorado school district, dated May 4, 2022, stating that her child's Private Information was compromised by the Data Breach. Ms. Weiland's children are minors who attend school in Colorado. Plaintiff is filing these claims as a real party in interest for herself and her minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

15. Plaintiff Kisil is a resident of New York. Ms. Kisil received a notice letter from the NYC Department of Education("NYCDOE") dated May 19, 2022, stating that her child's Private Information was compromised by the Data Breach. Ms. Kisil's child is a minor who attends school in New York. Plaintiff is filing these claims as a real party in interest for herself and her minor child pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

16. Plaintiff Chambers is a resident of California. Ms. Chambers received a notice letter from Illuminate dated July 29, 2022, stating that her child's Private Information was compromised by the Data Breach. Ms. Chambers' child is a minor who attends school in California. Plaintiff is filing these claims as a real party in interest for herself and her minor child pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

17. Plaintiff Vitro is a resident of California. Ms. Vitro's son received a notice letter from Illuminate dated July 29, 2022, stating that his Private Information was compromised by the Data Breach. Ms. Vitro's son is disabled, and she is his legal guardian and legal representative. Her son attended school in California. Plaintiff is filing these claims as a real party in interest for herself and her son pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

18. Plaintiff Deniz is a resident of California. Ms. Deniz received two notice letters from Illuminate dated July 15, 2022, stating that both of her children's Private Information was compromised by the Data Breach. Ms. Deniz' children are minors who attend school in California. Plaintiff is filing these claims as a real party in interest for herself and her minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C).

19. Defendant Illuminate Education, Inc., is a California corporation with its principal place of business in Irvine, California.

## JURISDICTION

20. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of different states than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Illuminate Education, Inc. because it is headquartered in California, is authorized to and conducts business in California, has specifically marketed, advertised, and made substantial sales in California, and has sufficient minimum contacts with this state and/or sufficiently avails itself of the markets of this state through its promotion, sales, and marketing within this state to render the exercise of jurisdiction by this Court permissible.

22. Venue in this Court is proper pursuant to 28 U.S.C. § 1391 because Defendant does substantial business in this District, has intentionally availed itself of the laws and markets within this District through its promotion, marketing, distribution and sales activities in this District, and a significant portion of the facts and circumstances giving rise to Plaintiffs' Complaint occurred in or emanated from this District.

## FACTUAL ALLEGATIONS

23. Illuminate touts that "[w]e protect your data like it's our own." Unfortunately for Plaintiffs and Class Members, nothing could be further from the truth. According to news reports, on January 8, 2022, Illuminate became aware that an unauthorized third party was able to gain access to databases of schools and had access to the personally PII[9] and protected health information (PHI") of the students (collectively, "Private Information") maintained by Illuminate .[10]

24. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[11] PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.*, as well as multiple state statutes.

25. However, it was not until March 24, 2022, that Illuminate announced that it "became aware of suspicious activity in a set of isolated applications within their program [and] immediately took steps to secure the affected applications and launched an investigation with external forensic specialists to determine the nature

[9] Personally identifiable information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual…The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. 2 C.F.R. § 200.79.

[10] *See* https://www.nydailynews.com/new-york/education/ny-hack-illuminate-online-gradebook-compromised-personal-data-20220325-ahy3b3b3t5cjzajau63muqcniq-story.html (last visited May 31, 2023); *see also* https://www.infosecurity-magazine.com/news/illuminate-breach-impacts-school/ (last visited May 31, 2023).

[11] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf. (last visited May 31, 2023).

*Footnote continued on next page*

and scope of activity."[12] [redacted]

26. Illuminate stated that its own investigation confirmed that "certain databases, containing potentially protected student information were subject to unauthorized access between December 28, 2021, and January 8, 2022" (the "Data Breach").[13] It took Illuminate over nearly 4 months to notify those affected by the Data Breach and in some cases has taken almost 6 months.

27. The Data Breach occurred after an attacker accessed systems operated by and/or for Illuminate, a software platform designed for K-12 school districts that allows educators to track and report on a number of attributes, including grades, attendance and class schedules, as well as to communicate with parents.[14] Such a hack was foreseeable due to the vast trove of valuable personal information on America's students contained therein and warnings from cybersecurity professionals.

28. Despite Illuminate's investigation finding that "certain databases, containing potentially protected student information" had taken place between December 28, 2021, and January 8, 2022, Illuminate did not notify schools of the breach until late March 2022 at the earliest.[15] In fact, some Plaintiffs' notification letters were dated July 29, 2022, over 4 months after Defendant purportedly concluded its investigation on March 24, 2022.

29. Cybercriminals unsurprisingly targeted a company in the business of storing sensitive personal information, including information protected by Family Educational Rights and Privacy Act ("FERPA"), [redacted]

[12] *See* https://www.bankinfosecurity.com/illuminate-education-mega-breach-impacts-k-12-students-a-19032 (last visited May 31, 2023).

[13] *Id.*

[14] *Id.*

[15] *See* https://www.infosecurity-magazine.com/news/illuminate-breach-impacts-school/ (last visited May 31, 2023).

[redacted].

30. [redacted]

31. In fact, Mayor Eric Adams of New York City stated that Illuminate's delay in formally informing the city of the Data Breach "shows the company has been more concerned with protecting itself than protecting our students".[16] "We will not tolerate bad actors in this city and plan to hold Illuminate fully accountable for not providing our students with the security and timely notification the company promised," Adams stated.[17]

32. [redacted][18]

[16] *See* https://www.nydailynews.com/new-york/education/ny-hack-illuminate-online-gradebook-compromised-personal-data-20220325-ahy3b3b3t5cjzajau63muqcniq-story.html (last visited May 31, 2023).

[17] *Id.*

[18] [redacted].

33. [redacted]

[redacted][19]

34. [redacted]

[redacted]

[19] *Id.*

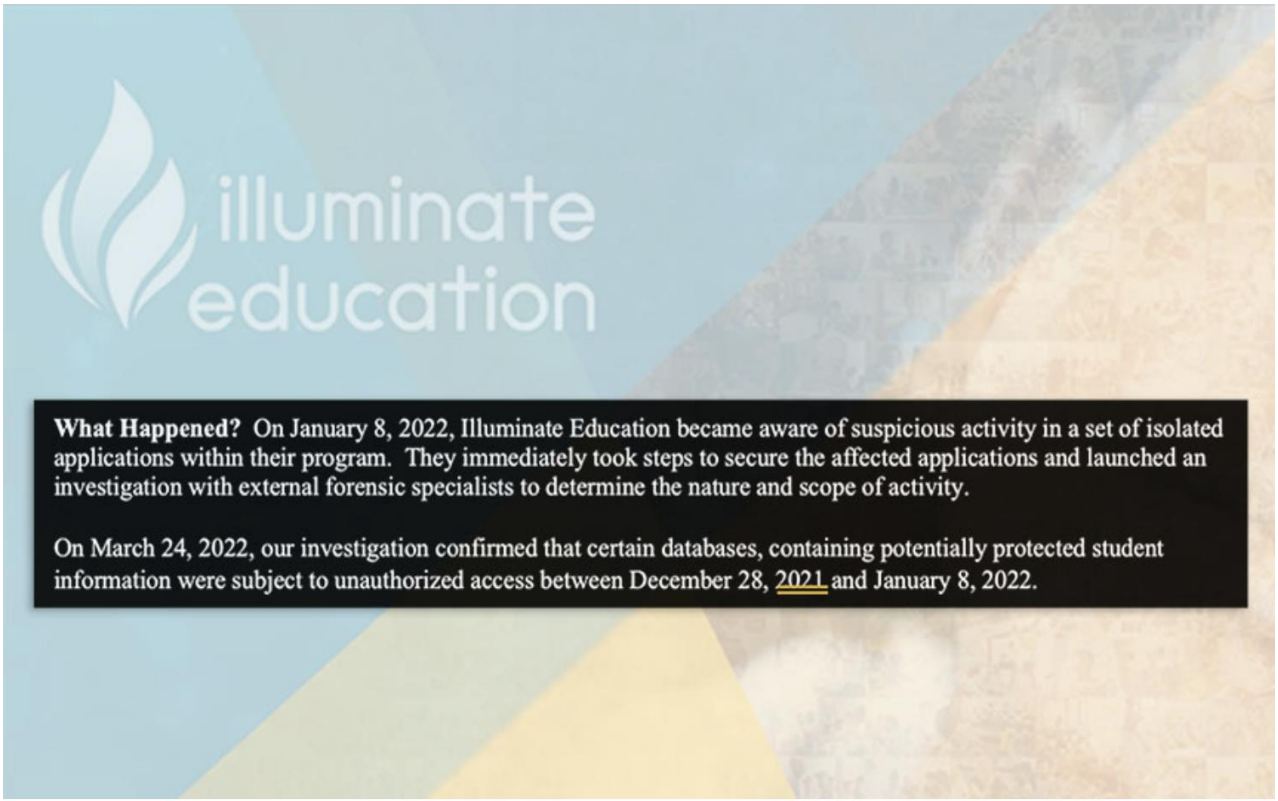
*Footnote continued on next page*

[redacted]”[20]

35. [redacted]

[redacted][21]

36. As revealed by a breach notification letter sent by one of the numerous, impacted school districts, [redacted], and the dates show a delay in notification:




Excerpt of a breach notification letter distributed by Colorado's Pueblo County School District 70 (Source: KOAA News5)

[20] *Id.*

[21] *Id.*

37. Based on news reports and other sources noted herein, the compromised files and data included both personal and medical information not limited to names, birthdates, ethnicities, home languages, and student ID numbers of current and former students going back to the 2016-17 school year.[22] Other information, such as whether students get special education services, class and teacher schedules, and whether kids receive free lunch was also disclosed.[23] Academic and behavior information was also disclosed.[24] Information such as this is immutable and highly sensitive.

38. According to reports, some districts and parents asked state and federal authorities to investigate the Data Breach, accusing Illuminate of failing to take the basic step of encrypting student data kept on its servers – even though the company had previously told the districts it was meeting such legal requirements for data protection.[25]

39. According to an expert who tracks school cybersecurity incidents, the Data Breach is likely the largest ever single breach of student data. In reference to the NYC school district, Doug Levin, the national director of K12 Security Information Exchange, stated "I can't think of another school district that has had a student data breach of that magnitude stemming from one incident".[26]

40. Defendant's failure to ensure that its services and products were adequately secure fell far short of its legal obligations and Plaintiffs' and Class Members' reasonable expectations for data privacy, jeopardized the security of their

[22] *Id*.

[23] *Id*.

[24] *See* https://www.infosecurity-magazine.com/news/illuminate-breach-impacts-school/ (last visited May 31, 2023).

[25] *See* https://thejournal.com/articles/2022/05/17/illuminate-data-breach-spreads-to-fifth-state-as-oklahoma-city-notifies-parents.aspx (last visited May 31, 2023).

[26] *See* https://www.nydailynews.com/new-york/education/ny-hack-illuminate-online-gradebook-compromised-personal-data-20220325-ahy3b3b3t5cjzajau63muqcniq-story.html (last visited May 31, 2023).

Private Information, violated applicable data privacy laws, and has put Plaintiffs' and Class Members at imminent risk of fraud and identity theft.

41. Illuminate, a for-profit company that earns revenue through government contracts paid by taxpayers, failed to disclose that its data systems were not secure and, thus, vulnerable to attack. Had this been disclosed, Illuminate would have been unable to continue obtaining business from school districts and it would have been forced to adopt and invest in reasonable data security measures and comply with the law. Illuminate pledged to protect the Private Information of current and former students but chose to ignore this pledge and the existing law by skimping on the security of its data systems. In fact, Illuminate retained former students' Private Information, for its own business purposes, longer than reasonably necessary and failed to encrypt this information or delete it. It also failed to put in place adequate and appropriate protocols for accessing the databases containing the information.

**B. Scope Of The Data Breach**

42. The Data Breach impacted students enrolled during the 2021-2022 school year in most cases but has also impacted at least some former students enrolled as far back as 2016.[27]

43. So far, the Data Breach has potentially affected well over 3 million former and current students. The Data Breach has affected some of the largest school districts in the nation which include districts in New York and California. In New York alone, hundreds of schools throughout the state have been affected and over 1.9 million students have had their Private Information disclosed.[28] School districts in Colorado, California, Oklahoma, Washington, and Connecticut have also been affected.[29] In California, over 500,000 students from dozens of school districts have

[27] *See* https://thejournal.com/articles/2022/05/15/list-of-all-schools-confirmed-impacted-by-illuminate-education-data-breach.aspx (last visited May 31, 2023).

[28] *Id.*

[29] *Id.*; *see also* https://thejournal.com/articles/2022/05/17/illuminate-data-breach-spreads-to-fifth-state-as-oklahoma-city-notifies-parents.aspx (last visited May, 2023); https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-

*Footnote continued on next page*

been affected by the Data Breach.[30] In Colorado, nine school districts with collectively over 140,000 students have been affected by the Data Breach.[31] In Washington, over 57,000 students have been impacted.[32] In Connecticut, four school districts with collectively over 10,000 students have been affected.[33] In Oklahoma, the Oklahoma City Public Schools with an enrollment of 34,000 students was affected.[34] Unfortunately for schools and students across the country, more districts continue to find out that they have been affected by the breach. In addition, these numbers may not include former students who are no longer enrolled in the schools but were impacted by the Data Breach. Plaintiffs allege that millions of students have been affected by this incident, from coast to coast in some of the largest school districts in the nation.[35]

44. In response to an email concerning the breach sent by Joanne Murphy, Data Visualization Designer at the Douglas County School District in Colorado, Adam Smith, Director of Customer Support at Illuminate stating that the scope of the highly sensitive and immutable nature of the information exposed and compromised by the Data Breach, included "Academic and Behavior" information concerning

techs-student-privacy-pledge-under-fire/ (last visited May 31, 2023).

[30] https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=1 (last visited May 31, 2023).

[31] *See* https://www.govtech.com/education/k-12/illuminate-education-data-breach-exposes-student-information (last visited May 31, 2023); *see also* (last visited May 31, 2023).

[32] *See* https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=6 (last visited May 31, 2023).

[33] *See* https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=2 (last visited May 31, 2023).

[34] *See* https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=6. (last visited May 31, 2023).

[35] *See* https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=1. (last visited May 31, 2023).

*Footnote continued on next page*

students and "Student Demographic Information."[36] This email was a summary of a formal letter that Illuminate claims they sent to the school on April 5, 2022, via First Class Mail that was not received as of the date of the email. As detailed below, per Mr. Smith's April 13 email, there was unauthorized access to Academic & Behavior Information, including but not limited to students' Graduation Status, GPA and Course Grades and behavior incidents, as well as sensitive and personal demographic information concerning students and their parents, including, but not limited to, students' birth city, socio-economic disadvantaged information, parents' highest level of education and parent home, work and cell numbers. Smith's email to Murphy states in part, the following:

> In summary of the letter, these were the impacted data categories for Douglas County School District (meaning we determined there was unauthorized access to data in the following categories):
>
> Student Data:
>
> **Academic and Behavior Information**
>
> **Student Demographic Information**
>
> Staff Data:
>
> **Demographic Information**
>
> For the above categories, here are the potentially affected fields within each category. Please note that not all students or staff will have information in every field – that depends on how your district was using the system:
>
> **Academic & Behavior Information**
> District Entry Date
> Gifted and Talented Indicator
> School Entry Date
> Graduation Date
> Graduation Status
> Graduation Service Hours
> State School Entry Date
> US School Entry Date

[36] Plaintiffs' counsel obtained a copy of the April 13, 2022 email from Adam Smith to Joanne Murphy in response to a Freedom of Information Act request.

Site ID
Next Site ID
Homeroom
College Bound Indicator
Enrollment Entry Date
Enrollment Entry Code
Enrollment Exit Date
Enrollment Exit Code
Student Grade Level ID
GPA
Weighted Cumulative GPA
Unweighted Cumulative GPA
Course Grades
Transcript Grades
Progress Grades
School Enrollment
Course Enrollment
Period and Teacher associations
Incident Type
Incident
Date

**Student Demographic Information**

Student ID
Ethnicity/Is Hispanic Indicator
Gender
Race
Primary Language Code
Correspondence Language Code
Birth City
Birth State
Birth Country
Residential Status Code
Military Family Indicator
Lunch ID
NSLP Indicator
Socio-Economic Disadvantage Indicator
Parent Highest Level of Education
Parent First Name
Parent Last Name
Parent Address 1
Parent Address 2

Parent City
Parent State
Parent Zip
Parent Cell Phone 1
Parent Cell Phone 2
Parent Home Phone 1
Parent Home Phone 2
Parent Work Phone 1
Parent Work Phone 2

45. Due to the extent and severity of the Data Breach, New York City officials were outraged by the Data Breach and asked the New York attorney general's office and the F.B.I. to investigate (while doing their own investigation) and instructed New York City schools to stop using Illuminate. New York City Mayor Eric Adams stated that "Our students deserved a partner focused on having adequate security, but instead their information was left at risk."[37] Mayor Adams further stated that his administration was working with regulators "as we push to hold the company fully accountable for not providing our students with the security promised."[38]

46. [redacted]

[37] *See* https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html?searchResultPosition=7k. (last visited May 31, 2023).

[38] *Id.*

[redacted] [39]

47. According to a New York Times article dated July 31, 2022 on the Data Breach, (as well as other sources) "Illuminate kept student data on the Amazon Web Services online storage system." Astonishingly, the same article noted that after the Data Breach and after Illuminate made representations that it was working with outside experts to investigate the security incident and had made numerous security upgrades and instituted third-party monitoring on all of its Amazon Web Services ("A.W.S.") databases, that Greg Pollock, the vice president for cyber research at UpGuard, a cybersecurity risk management firm, during an interview on the Illuminate Data Breach, was able to find one of Defendant's A.W.S. buckets with an easily guessable name and the reporter interviewing Pollock was able to find a second A.W.S. bucket.

**2.** [redacted]

48. Sophisticated companies like Illuminate are aware of the different types of threat actors acting across the Internet and the type of security scams they employ for profit. Accordingly, it is imperative that, as a company specializing in and profiting from providing data security services to others, it guards against such attacks.

49. [redacted]

[39] [redacted]

50. [redacted]

51. [redacted]

52. [redacted]

53. [redacted]

54. [redacted]

[40] [redacted]

[41] [redacted]

[42] [redacted]

[43] [redacted]

[44] [redacted]

*Footnote continued on next page*

55. [redacted]

56. [redacted]

57. [redacted]

58. [redacted]

tes

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

*Footnote continued on next page*

[redacted]

59. [redacted]

[redacted]

60. [redacted]

[redacted]

61. [redacted]

[redacted]

62. [redacted]

[redacted]

[redacted]

50 [redacted]

51 [redacted]

52 [redacted]

63.

64. [redacted]

65. [redacted]

66. [redacted]

[53] [redacted]

[54] [redacted]

[55] [redacted]

[56] *See, e.g.,* [redacted]

[57] [redacted]

*Footnote continued on next page*

67. [redacted]

68. [redacted]

69. [redacted]

**C. Illuminate's Privacy Policies**

70. Defendant promised to protect the Private Information and other data of current and former students in the various and several school districts, in accordance with the applicable Federal, State and local statutes and regulations, emphasizing its

[redacted]

58 [redacted]

purported commitment to protection of Private Information and other data on its website, contracts with school districts, the Pledge (discussed below), and elsewhere.

71. Defendant's website claims:

> We protect your data like it's our own. In alignment with the Family Educational Rights and Privacy Act (FERPA), we deploy meaningful safeguards to protect student data.
>
> We pledge our unwavering commitment to student data privacy.
>
> We aim to give educators the confidence that all your data remains secure when you use our site and services.
>
> Whether collected directly from our Website or maintained on behalf of your Educational Organization, protecting the privacy of your information is important to us. We take security measures—physical, electronic, and procedural—to help defend against the unauthorized access and disclosure of your information. In addition to the restrictions discussed in this Privacy Policy, our employees are required to comply with information security safeguards, and our systems are protected by technological measures to help prevent unauthorized individuals from gaining access. The specific measures Illuminate takes to secure your information are defined by the contract between Illuminate and your Educational Organization. These measures meet or exceed the requirements of applicable federal and state law. Illuminate's employees are trained to observe and comply with applicable federal and state privacy laws in the handling, processing, and storage of your information.[59]

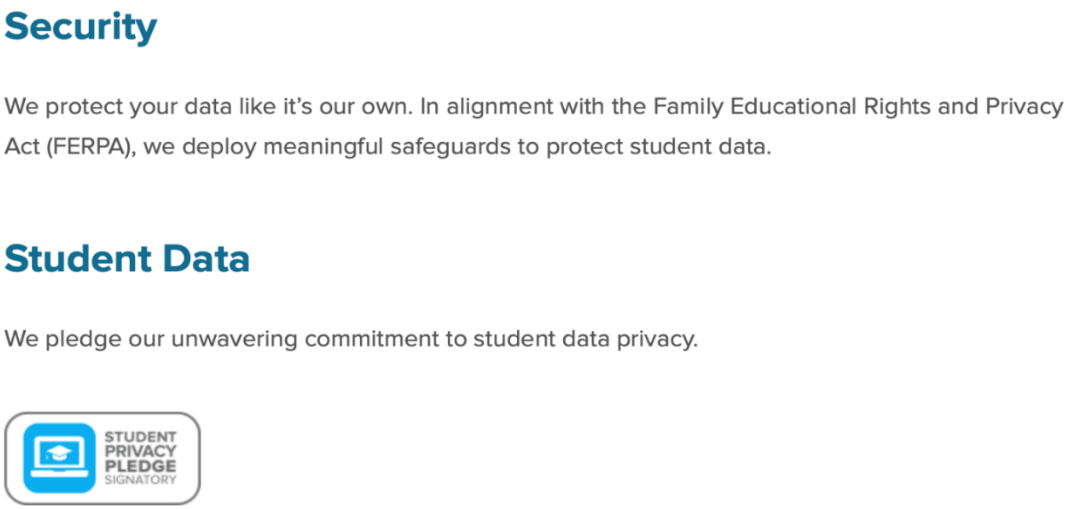
72. In fact, in February of 2016, Illuminate signed a pledge to respect student data privacy and to safeguard student information. The Student Privacy Pledge (the "Pledge") which was created in 2014 by the Future of Privacy Forum ("FPF") "incorporates the importance of protecting student personal data."[60]

[59] *See* https://www.illuminateed.com/resources/security-privacy/. (last visited May 31, 2023).

[60] *See* Illuminateed.com/blog/2016/02/illuminate-signs-student-privacy-pledge/. (last visited May 31, 2023).

73. When a company takes this pledge, they are "making a public statement of their practices with respect to student data…" The Student Privacy Policy Website states that "If a company acts in contradiction to their own public statements, they risk an enforcement action for 'unfair or deceptive trade practices.' This is known as FTC Section 5 authority, which you can learn more about by visiting the FTC's explanation."[61]

74. Illuminate promised that it would protect students' Private Information and failed to do so. On its website, it states that "Illuminate stores such information in locations outside its facilities, such as on servers…or with secure cloud-storage services"[62]:




75. Illuminate prides itself on an "unwavering commitment to student data privacy" and promises to "deploy meaningful safeguards to protect student data."

76. In signing the Pledge, Illuminate represented to students and parents that it would, (1) provide "a secure online environment with data privacy securely in place."; and (2) promote "that student data be safeguarded…" Additionally, Illuminate states that "Sharing that Illuminate has signed the Student Privacy Pledge

[61] *See* https://thejournal.com/articles/2022/08/09/illuminate-education-booted-from-student-privacy-pledge-referred-for-potential-ftc-state-ag-action.aspx. (last visited May 31, 2023).

[62] *See* https://www.illuminateed.com/resources/security-privacy/. (last visited May 31, 2023).

*Footnote continued on next page*

will give parents and educators confidence that data privacy safeguards are in place when using Illuminate!"[63]

77. In fact, on August 8, 2022, the FPF announced that it had removed Illuminate from the nonprofit's list of Student Privacy Pledge signatories as a result of the Data Breach.[64] This was the first time a company had been de-listed from the Pledge.[65]

78. The FPF had conducted a review of whether Illuminate's data practices meet the requirements of the Student Policy Pledge and found "those practices lacking." [66]

79. In addition, the FPF informed the NYAG of several failures by Illuminate to provide information to the FPF which included the following:

> FPF's review included direct outreach to Illuminate Education. In multiple communications with Illuminate, the company would not state that it encrypted all student information while at rest and in transit during the relevant time periods.[67]

80. The FPF also informed the NYAG that "Illuminate did not provide any meaningful non-public information to FPF during [FPF's] review".[68]

81. The FPF stated that "Publicly available information appears to confirm that Illuminate Education did not encrypt all student information while at rest and in transit." This failure to encrypt the student records violate the following Pledge commitments to:

> "maintain a comprehensive security program that is

---

[63] *Id.*

[64] *See* https://thejournal.com/articles/2022/08/09/illuminate-education-booted-from-student-privacy-pledge-referred-for-potential-ftc-state-ag-action.aspx (last visited May 31, 2023).

[65] *Id.*

[66] *See* Illuminate Education Booted from Student Privacy Pledge, Referred for Potential FTC and State AG Action -- THE Journal. (last visited May 31, 2023).

[67] FPF-000208.

[68] *Id.*

> reasonably designed to protect the security, confidentiality, and integrity of Student PII - such as unauthorized access or use, or unintended or inappropriate disclosure - through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information; and
>
> "comply with applicable laws," including New York state law that explicitly requires data encryption. FPF noted that throughout "multiple communications with Illuminate, the company would not state that it encrypted all student information while at rest and in transit during the relevant time periods."[69]

82. In light of regulations about how children's Private Information is collected and maintained, the companies providing the service of collecting and maintaining such information purport to understand this critical concern about the safe keeping of children's data.

83. Illuminate touted its security, but it would not even verify to the FPF that Illuminate had taken the most basic protective action of encrypting the data. Illuminate signed the Pledge, violated it, and refused to cooperate with FPF in an investigation. The logical conclusion from Illuminate's response to the FPF is that Illuminate did not want the full extent of its violations of the Pledge to come to light.

**D. Illuminate's Responsibility to Safeguard Information**

84. Beyond the obligations created in its security and privacy policies, Illuminate owed Plaintiffs and class members a duty to safeguard their Private Information.

85. First, as described further below, Illuminate owed a duty to safeguard Private Information pursuant to a number of statutes, including the HIPAA, the Federal Trade Commission Act ("FTC Act"), Children's Online Privacy Protection Act ("COPPA"), Family Educational Rights and Privacy Act ("FERPA") and the

[69] *Id.*

New York Education Law ¶2-d to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and the class members from the type of conduct by Illuminate alleged herein.

86. Next, Illuminate owed a duty to safeguard Private Information, given that it was on notice that it was maintaining highly-valuable data, for which Illuminate knew there was a risk that it would be targeted by cybercriminals. Illuminate knew of the extensive harm that would occur if Plaintiffs' and class members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

87. Given the sensitive nature of the Private Information obtained by Illuminate, Illuminate knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud if it were able to exfiltrate that data from Illuminate's servers. Illuminate also knew that individuals whose Private Information was stored on Illuminate's servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

88. Illuminate also owed a duty to safeguard Plaintiffs' and class members' data based upon the promises that it made to Plaintiffs' and class members' to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. Illuminate voluntarily undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and class members to keep their Private Information secure.

89. Illuminate also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—it did not do.

### E. Illuminate Failed to Meet Its Obligations to Protect Private Information or Comply with its own Privacy Policies

90. Illuminate's services are supported by privacy policies and purported security practices, which it provides on a publicly-facing website.

91. Illuminate was keenly aware of the obligations that state and federal law imposed upon it given the types of information that Illuminate stored and processed for Plaintiffs and class members.

92. Illuminate also had a special relationship with Plaintiffs and class members from being entrusted with their Private Information, which provided an independent duty of care. Illuminate had a duty to use reasonable security measures because it undertook to collect, store and use consumers' Private Information. Regardless of whether the information was provided to Illuminate by their schools as part of a vendor agreement, Illuminate owed a duty to protect and safeguard that Private Information.

93. Illuminate has further failed Plaintiffs and class members by its failure to maintain a comprehensive and sufficient security program, including by not adequately securing and protecting Private Information that was stored on its systems.

94. Illuminate failed to provide Plaintiffs and Class Members with timely and adequate notice of the extent of the Data Breach. Timely notification of the breach was required so that, among other things, Plaintiffs and Class members could take measures to freeze or lock their minor's credit profiles, enroll in credit monitoring services, monitor their minor's account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, and take other steps to try to prevent identify theft. [redacted]

[redacted]

[redacted]

[redacted]

### F. Illuminate Failed to Comply with Industry and Regulatory Standards

95. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining, and securing Private Information,

such as Illuminate, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; protection against any possible communication system; and training staff regarding critical points.[70]

96. Further, federal and state governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions.

97. Illuminate was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in unfair or deceptive acts or practices in or affecting commerce. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

98. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

99. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer

[70] *See White Paper: Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/. (last visited May 31, 2023).

needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

100. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

101. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

102. Illuminate also had a duty to safeguard Plaintiffs' and class members' PHI under HIPAA and its implementing regulations, 45 C.F.R. §§ 160, et seq., which establish privacy and security standards for certain health organizations and their "business associates." Illuminate is a "business associate" subject to HIPAA because it receives, maintains, or transmits its customers' PHI.[71] "PHI" includes, in relevant part, individually identifiable health information relating to the provision of health care.

103. For example, HIPAA required Illuminate to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id.* § 160.306(a). To do so, Illuminate was required to implement reasonable and appropriate security measures to mitigate the risk of

[71] 45 C.F.R. § 160.103.

*Footnote continued on next page*

unauthorized access to its customers' electronic personal health information, including by encrypting certain data where appropriate.[72]

104. Illuminate failed to properly implement these basic data security practices. Illuminate's failure to employ reasonable and appropriate measures to protect against unauthorized access to students' Private Information, including HIPAA-related Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

**G. Illuminate's Failures Resulted in a Data Breach**

105. [redacted], Plaintiffs and class members provided sensitive and personally identifying Private Information to Illuminate through their schools. When providing such information, Plaintiffs and class members reasonably expected that the manager and securer of their Private Information, Illuminate, would maintain security against cybercriminals and cyberattacks.

106. Illuminate maintained Plaintiffs' and the class members' data on its systems. Despite its own awareness of steady increases of cyberattacks on schools, health care providers and other facilities over the course of recent years, Illuminate did not maintain adequate security of Plaintiffs' and the class members' Private Information and did not adequately protect it against hackers and cyberattacks.

107. [redacted].[73]

108. [redacted]

[72] *See id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

[73] https://ecfirst.com/wp-content/uploads/2023/02/ecfirst-Services-Detailed-Brochure_23A.pdf. (last visited May 31, 2023).

[redacted]”[74]

109. [redacted]

[redacted]

110. [redacted]

[74] ILLUM_00003716-0003777.
[75] Id.
[76] ILLUM_00004144-00004298.
[77] ILLUM_00003722.
[78] Id.
[79] ILLUM_0003723.
[80] *Id*.

*Footnote continued on next page*

111. [redacted]

112. [redacted]

113. [redacted]

[81] *Id.*

[82] *Id.*

[83] ILLUM_00003661-00003715.

[84] ILLUM_00003017-00003190.

[85] ILLUM_00003669.

[86] ILLUM_00003024-00003026.

[redacted]

114. [redacted]

[redacted]

115. [redacted]

116. [redacted]

117. [redacted]

### H. Data Breaches Put Consumers at Increased Risk of Fraud and Identity Theft

118. The Data Breach creates a heightened security concern for students and parents who use Illuminate because their Private Information, including unique academic records and other sensitive financial and personal data was included.

119. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[87] America's largest corporations profit almost exclusively through the use of

[87] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm. (last visited May 31, 2023).

Private Information illustrating the considerable market value of personal Private Information.

120. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can [redacted], use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

121. [redacted]

122. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

123. Cyberattacks and data breaches of medical facilities, educational and religious institutions, and non-profit entities are especially problematic because of the disruption they cause to the daily lives of the patients, students, donors, and other

individuals affected by attack, including minor children and adults lacking capacity to consent to the disclosure of their information.

124. It must also be noted there may be a substantial time lag-measured in years- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. [88]

125. Private Information is such an inherently valuable commodity to identity thieves that, once compromised, criminals often trade the information on the cyber black-market for years.

**Minors' Private Information is Particularly Valuable and the Harm to a Minor Resulting from a Breach is Significant**

126. Students' and children's privacy is very important. Indeed, numerous state and federal laws safeguard it. Furthermore, students and children are more vulnerable to identity theft and other consequences of their Private Information falling into the wrong hands because they are less likely to regularly monitor this information.[89]

127. Defendant's conduct is particularly egregious because some education vendors typically do not know a whole lot about the students they're serving. In one

[88] Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 29, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf. (last visited May 31, 2023).

[89] *See* https://www.credit.com/personal-finance/use-credit-monitoring-protect-childs-identity/ (last visited May 18, 2023).

*Footnote continued on next page*

interview, a cybersecurity expert stated that "[t]he Illuminate Education breach did involve a pretty large swath of sensitive information about students that could be used by criminals to commit identity theft and credit fraud against students."[90] Importantly, students and their families were required to engage with Illuminate's software and provide Illuminate with their Private Information in order to simply obtain their education, distinguishing this case from commercial data breaches involving adult consumers, who can be more discerning about whether and how to provide financial or personal information to companies when shopping or traveling.[91]

128. [redacted]

129. It is well known that personal information of children of the type stolen by data thieves from Illuminate, is particularly attractive to cyber criminals and identity thieves who know there is a valuable market for such information. In fact, in its report entitled *The State of K-12 Cybersecurity: 2018 Year in Review*, The K-12 Cybersecurity Resource Center noted that nearly a quarter of "data breach incidents

[90] *See* https://www.the74million.org/article/74-interview-cybersecurity-expert-levin-on-the-harms-of-student-data-hacks/ (last visited May 31, 2023).

[91] *Id.*

[92] [redacted]

*Footnote continued on next page*

were carried out by unknown actors, often external to the school community and for malicious purposes (such as identity theft)."[93] The report further noted that "security researchers have documented dark web marketplaces advertising the stolen information of children for use by identity thieves. Indeed, student data breaches can have serious and long-lasting consequences." [94]Children's data is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity. Specifically:

> The theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to go to college and start applying for student loans or get their first credit card. By then, the damage is done and the now young adult will need to go through the pain of proving that their identity was indeed stolen.[95]

130. The serious financial and other harm to students from disclosure of their PII and/or names and birthdates, not to mention the other types of sensitive personal information of the type stolen in this case, such as individualized education programs, special education and behavioral information, cannot be overstated. These harms were recognized in a September 2020 Report by the United States Government Accountability Office ("GAO") on Data Security entitled *Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*.[96] Indeed, the GAO's Report noted that:

> Access to or disclosure of some of the types of data collected by K-12 institutions can harm students, including their

[93] https://k12cybersecure.com/wp-content/uploads/2019/02/K12Cybersecurity-2018YIR-1.pdf. (last visited May 31, 2023).

[94] Id.

[95] Avery Wolfe, *How Data Breaches Affect Children*, AXIOM Cyber Solutions (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/. (last visited May 31, 2023).

[96] GAO-20-644 Student Data Security

> financial well-being. According to our analysis of CRC data, 22 of the 36 reported breaches that exposed students' PII included full or partial Social Security numbers, **or names and birthdates**. Financial and cybersecurity experts say this kind of information can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood. Data breaches can **also cause students physical and emotional harm…** For example, for students with an Individualized Education Program (IEP), disclosure of special education status, annual goals, or medical diagnoses contained in these records could lead to embarrassment or stigmatization. (emphasis added)[97]

131. The disclosure of students' Private Information that is part of this Data Breach such as mental health issues, behavioral issues and disabilities can not only cause embarrassment or stigmatization to a student but can negatively affect their ability to get into college or secure employment in the future.

132. In 2011, Carnegie Mellon University's CyLab reported "the rate of child identity theft is 51 times higher than for adults (whose data sets cost about $10 - $25 on dark web markets)."[98]

133. By early 2018, it became well known that the data of infants was being sold on the dark web. As of 2018, the cost of an infant's data was approximately $300 in Bitcoin, which would "provide cybercriminals access to a clean credit history."[99]

134. As one cyber-security author further explained, the impact of the use of children's information is further exacerbated by the fact that there are few checks on

[97] The type of sensitive and particularized Private Information stolen here could also be used by child predators to gain the trust of their unsuspecting targets.

[98] Selena Larson, *Infant Social Security Numbers Are for Sale on the Dark Web*, CNN Bus. (Jan. 22, 2018), https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html. (last visited May 31, 2023).

[99] *Id.*

*Footnote continued on next page*

using a child's data to initially obtain credit and slowly increase it over time-all while being undetected by the child and the parents.[100] Thus, "[t]he problem goes unnoticed for years-possibly decades-before the child goes to apply for student loans, open their first credit card, or buy their first car."[101]

135. In particular, the exposure of the PII in this Breach could have long term consequences. Joe Green, a cybersecurity professional and parent of one of the Colorado high school students whose information was stolen stated: "If you're a bad student and had disciplinary problems and that information is now out there, how do you recover from that?... It's your future. It's getting into college, getting a job. It's everything."[102]

136. In fact, parents of students who were affected by the Data Breach were outraged and extremely concerned about the exposure of their children's Private Information. One parent of a Douglas County student stated in an email to the Douglas County School District that "[o]ne of [his] main concerns is the types of data Illuminate outlined as the breached data could be used to gain student credentials with a very high success rate."[103] He found the responses and offers for "identity monitoring services" not to be satisfactory.[104]

137. Another Douglas County School District parent of a student was "outraged at the breach" and noted that there were "ethical issues", "no transparency" and issues related to the deletion of student data.[105]

---

[100] *See* Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/. (last visited May 31, 2023).

[101] *Id*.

[102] *See* https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html?searchResultPosition=7k. (last visited May 31, 2023).

[103] DCSD00179.

[104] *Id*.

[105] DCSD005358.

*Footnote continued on next page*

138. Another parent who is a cybersecurity architect for a large global bank and investment firm stated his concerns about the Private Information exposed during the Data Breach; believed that more than twelve months of credit protection was warranted.[106]

139. These are just a few examples of parents' complaints out of the many received by the Douglas County School District and it is likely that each school district affected by the Data Breach had many concerns expressed to them by the parents as well.

## I. Plaintiffs and Class Members Suffered Damages

139. Defendant had a duty to keep Private Information confidential and to protect it from unauthorized access and disclosures. Plaintiffs and Class Members provided their Private Information to Illuminate with the understanding that Illuminate and any business partners to whom Illuminate disclosed Private Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

140. In addition, Illuminate owed a duty to safeguard Private Information pursuant to a number of statutes, including the HIPAA, the Federal Trade Commission Act ("FTC Act"), Children's Online Privacy Protection Act ("COPPA"), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and the class members from the type of conduct by Illuminate alleged herein.

140. Defendant's data security obligations were particularly important given the substantial increases in data breaches in recent years, which are widely known to the public and to anyone in Illuminate's industry of data collection and transfer.[107]

[106] DCSD000882.

[107] *See* https://marketbrief.edweek.org/marketplace-k-12/pearson-will-pay-1-million-fine-understating-2018-data-breach-misleading-investors/ (last visited May 31, 2023).

141. Data breaches are not new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks. Indeed, Pearson Education recently paid $1 million in fines for failing to properly disclose information about its data breach.[108]

142. It is well known among companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals and that they need to implement appropriate security measures to keep criminals from accessing Private Information.

143. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud. This is particularly true of children's personal information, because they are less likely to conduct regular credit monitoring and their information is more likely to be on the "dark web."[109]

144. There may be a time lag between when the harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According, to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[110]

---

[108] *Id.*

[109] *See* https://www.kqed.org/news/11898753/experts-say-you-should-freeze-your-childrens-credit-heres-how (last visited May 31, 2023).

[110] *Report to Congressional Requesters*, U.S. Government Accountability Office, (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last visited May 31,

*Footnote continued on next page*

145. With access to an individual's Private Information, criminals can commit all manners of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture, or filing a fraudulent tax return using the victim's information.

146. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Private Information directly on various illegal websites making the information publicly available, often for a price.

147. Illuminate is, and at all relevant times has been, aware that the sensitive Private Information it handles and stores in connection with providing its services is highly sensitive. As a company that provides services involving highly sensitive and identifying information, Illuminate is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

148. Illuminate was also aware, or should have been aware, of regulatory and industry guidance regarding data security.

149. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable data breaches, Defendant failed to take reasonable steps to adequately protect its systems from being breached and to properly secure its platforms, leaving its clients and all persons who provide sensitive Private Information to its clients exposed to risk of fraud and identity theft.

150. In addition, the Data Breach was the result of Illuminate's failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove old unused and no longer needed data of former students containing Private Information or to encrypt such information. Illuminate, in fact, had no valid business reason for retaining such

---

2023).

records containing highly sensitive Private Information for such long periods and for failing to delete or encrypt such information.

151. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; disclosure of their need for special education; disclosure of financial status; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Private Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Private Information.

152. As a result of the Data Breach, Plaintiffs' and Class Members' privacy has been invaded, their Private Information is now in the hands of criminals, they face a substantially increased risk of identity theft, fraud and other harms, and they must take immediate and time-consuming action to protect themselves from such.

153. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

154. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft, fraud, and other harms requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

155. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[111]

156. In the Data Breach Notice, Illuminate made an offer of identity monitoring service to students whose data was compromised. Illuminate has not offered or provided victims any fraud insurance or medical identity theft protection. Illuminate's offer fails to address the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and potentially other harms (particularly given the sensitivity of the Private Information of minor students at issue here) and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

157. Other than providing 12 months of credit monitoring, Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members other than telling them to simply do the following:

- "remain vigilant for incidents of identity theft and";
- "review[] your minor's account statements and monitor[] your free credit reports for suspicious activity";
- Place a security freeze on your minor's credit file;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- place a fraud alert on your minor's credit report.

[111] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf ((last visited May 31, 2023).

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class Members' Private Information, and put the onus on Plaintiffs and Class Members to expend time, money, and energy to complete these tasks.

158. Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money - while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Illuminate's Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

159. Illuminate's offer of 12 months of identity monitoring to Plaintiffs and Class Members is woefully inadequate, while at the same time serving as a stark admission that Plaintiffs and members of the Class face a heightened risk of identity theft and/or other harms as a result of the Data Breach. While some harm has begun already, the worst is likely yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) - it does not prevent identity theft.[112]

160. Plaintiffs and Class Members have been damaged in several other ways as well. All Plaintiffs and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of

[112] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited May 31, 2023).

their Private Information, which is why Illuminate advised Plaintiffs and Class Members to take the various measures noted above. Plaintiffs and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Certain Plaintiffs and Class Members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class Members also suffered a loss of the inherent value of their Private Information.

161. PII stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

162. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching

how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their Private Information.

163. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

### J. Illuminate's Delay in Identifying & Reporting the Breach Caused Additional Harm

164. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[113]

165. Indeed, once a data breach has occurred:

> One thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on

[113] https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-with-15.4-Million-U.S.-Victims-in-2016-Up-16-Percent-According-to-New-Javelin-Strategy-Research-Study. (last visited May 31, 2023).

> credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[114]

166. Although their Private Information was improperly exposed between on or about December 28, 2021, and January 8, 2022. Defendant began notifying Plaintiffs and Class Members of the Data Breach in mid-April 2022. However, many Plaintiffs and Class Members did not receive the notice letter until the end of July 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

167. [redacted]

168. The earliest notification by Defendant to the California Attorney General was not until May 13, 2022, with additional notifications after that date and as late as July 29, 2022.[115] Defendant did not notify the New York City school district

[114] https://www.consumerreports.org/data-theft/the-data-breach-next-door-a7102554918/. (last visited May 31, 2023).

[115] *See* https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=Illuminate&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last visited May 31, 2023).

*Footnote continued on next page*

of the Data Breach until March 25, 2022[116] and did not notify the Washington Attorney General until April 22, 2022, with additional notifications after that date and as late as August 2, 2022.[117]

169. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, [redacted], the risk of fraud and other harms for Plaintiffs and Class Members has been driven even higher.

170. In addition, in August 2022, Renaissance Learning ("Renaissance"), which holds itself out as a global leader in pre-k to 12 education technology, acquired Illuminate for an undisclosed purchase price. In a letter sent to Illuminate customers on or about August 24, 2022 sharing the news about the acquisition, Renaissance's CEO, Chris Bauleke, noted the data breach experienced by Illuminate earlier in the year. [redacted] While the potentially protected student information was isolated to two Illuminate products (Data Driven Classroom, IO Assessment) and one tool (IO Admin) used to transfer data to or from other products, we understand that an incident of this kind causes concern."

[116] *See* https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html (last visited May 31, 2023).

[117] *See* https://www.atg.wa.gov/search/node/Illuminate%20type%3Adata_breach_notification (last visited May 31, 2023).

**K. Plaintiffs' Experiences**

171. Plaintiff **Lucas Cranor** is a resident of Colorado. Plaintiff is filing these claims as a real party in interest for himself and his minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C). Mr. Cranor received two notice letters from Illuminate dated April 29, 2022, stating that both of his children's Private Information was compromised by the Data Breach. Mr. Cranor's children are minors who attend school in the Douglas County School District in Colorado.

172. In the letter, Defendant stated that it "is now notifying you of this incident because our investigation has determined that your minor's information was contained in the affected databases." The letter went on to disclose that "[t]he affected databases may have contained the following: your minor's name, student identification number, academic and behavior information, enrollment information, accommodation information, special education information, and/or student demographic information."

173. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, corresponding with Illuminate and making public records requests concerning the Data Breach, exploring credit monitoring and identity theft insurance options and monitoring his children's information. To date, Plaintiff has spent at least 36 hours dealing with the Data Breach.

174. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information - a form of intangible property that Plaintiff entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach.

175. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mr. Cranor otherwise

would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

176. Knowing that thieves stole his children's Private Information, potentially including their PHI and other immutable information, and knowing that his children's Private Information may be available for sale on the dark web, has caused Plaintiff Cranor emotional distress. He is now very concerned about identity theft in general.

177. Plaintiff has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals. In addition, Plaintiff Cranor has noticed a substantial uptick in unwanted spam telephone calls and emails since the Data Breach.

178. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned that his children's Social Security numbers, which were part of their student records at the time of the breach, may have been breached as well.

179. On information and belief, Plaintiff believes that his Private Information including his name, address, phone number and email may have been breached as well because it is part of his children's school records. This is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne Murphy, the Data Visualization Designer at Douglas County School District in Colorado which is the school district that Plaintiff Cranor's children attend.[118]

180. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

[118] See ¶ 44 above.

181. Plaintiff **Kristen Weiland** is a resident of Colorado. Plaintiff is filing these claims as a real party in interest for herself and her minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C). Ms. Weiland received one or more notice letters from the Douglas County, Colorado school district, dated May 4, 2022, stating that her child's Private Information may have been compromised by the Data Breach. Ms. Weiland's three children are minors who were enrolled at schools in the Douglas County School District in Colorado.

182. The letter stated in part that "Illuminate Education recently informed us that some of their products were affected by a data security incident. Illuminate has determined that an unauthorized third party gained access to a dataset containing student information belonging to schools and school districts nationwide. **Illuminate has indicated that your student's data may have been affected**." (emphasis in original).

183. Plaintiff Weiland suffered actual injury in the form of damages to and diminution of the value of Private Information - a form of intangible property that Plaintiff entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach. Two of Plaintiff's children have special needs which makes them even more vulnerable since their school records contain extremely sensitive information.

184. Plaintiff Weiland has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Weiland otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

185. Knowing that thieves stole her children's Private Information, potentially including their PHI and other information, and knowing that her children's Private Information may be available for sale on the dark web, has caused Plaintiff Weiland emotional distress. She is now very concerned about identity theft in

general, and what could happen to her children in the future because of the Data Breach.

186. Plaintiff Weiland has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals. In addition, Plaintiff Weiland has noticed a substantial uptick in unwanted spam telephone calls and text messages since the Data Breach.

187. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned that her children's Social Security numbers, which were part of their student records, at the time of the breach may have been breached as well.

188. Further, Plaintiff Weiland is concerned that her children's medical and behavioral histories that are both part of their student records have been breached as well.

189. On information and belief, Plaintiff Weiland believes that her Private Information including her name, address, phone number and email may have been breached as well because it is part of her child's school records. This is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne Murphy, the Data Visualization Designer at Douglas County School District in Colorado which is the school district that Plaintiff Weiland's children attend.[119]

190. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

191. Plaintiff **Anastasiya Kisil** is a resident of New York. Plaintiff is filing these claims as a real party in interest for herself and her minor child pursuant to

[119] See ¶ 44 above.

Federal Rule of Civil Procedure 17(a)(1)(C). Plaintiff Kisil received a notice letter from the NYC Department of Education("NYCDOE") dated May 19, 2022, stating that her child's Private Information was compromised by the Data Breach. Ms. Kisil's child is a minor who attends school in New York.

192. The letter stated that the Defendant informed the NYCDOE that "… its investigation has determined that your child's information was contained in the affected databases." The letter went on to disclose that "[t]he affected databases contained the following information about **all** affected NYCDOE students, including your child: first and last name, student identification number, and school." "…. At least two of the following information items for **all** affected NYCDOE students, including your child: **date of birth**, gender, grade level, **race/ethnicity**, home language, and class information (including teacher name and/or subject)." (emphasis in original).

193. In addition, the letter also stated that "the affected databases contained academic testing information, including scores and answers for **some** NYCDOE students. Your child had such information affected." The letter also stated that "the affected databases contained one or more of the following pieces of information for some NYCDOE students: whether the student is an English Language Learner, whether the student receives special education services (but not information on the services themselves or the content of the Individualized Education Plans), and (for a very small number of students) whether the student is economically disadvantaged. Your child had such information affected."

194. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, researching and signing up for credit monitoring offered by Defendant and monitoring her child's information. To date, Plaintiff has spent at least 15 hours dealing with the Data Breach.

195. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach.

196. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Kisil otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

197. Knowing that thieves stole her child's Private Information, potentially including their PHI and other immutable information, and knowing that her child's Private Information may be available for sale on the dark web, has caused Plaintiff Kisil emotional distress. She is now very concerned about identity theft in general, and what could happen to her child in the future because of the Data Breach.

198. Plaintiff has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

199. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned that her son's Social Security number, which was part of his student records at the time of the breach, may have been breached as well.

200. In addition, Plaintiff is concerned that her son's medical history that is part of his student records has been breached as well.

201. On information and belief, Plaintiff believes that her Private Information including her name, address, phone number and email may have been breached as well because it is part of her child's school records. The likelihood that Plaintiff's Private Information was part of the Data Breach is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne

Murphy, the Data Visualization Designer at Douglas County School District in Colorado.[120]

202. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

203. Plaintiff **Tara Chambers** is a resident of California. Plaintiff is filing these claims as a real party in interest for herself and her minor child pursuant to Federal Rule of Civil Procedure 17(a)(1)(C). Ms. Chambers received a notice letter from Illuminate dated July 29, 2022, stating that her child's Private Information was compromised by the Data Breach. Ms. Chambers' child is a minor who attends school in the Apple Valley Unified School District in California.

204. In the letter, Defendant stated that it "is now notifying you of this incident because our investigation has determined that your minor's information was contained in the affected databases." The letter went on to disclose that "[t]he affected databases may have contained the following: your minor's name, academic and behavior information, enrollment information, accommodation information, special education information, medical information, and/or student demographic information."

205. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, researching and signing up for credit monitoring offered by Defendant, researching credit freezes for her child's credit and monitoring her child's information. To date, Plaintiff has spent at least six hours dealing with the Data Breach.

206. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information - a form of intangible property that Plaintiff

[120] *See* ¶ 44 above.

entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach.

207. In addition, since the Data Breach, Plaintiff's son has experienced an increase in spam text messages on the phone number that he had provided to the school. Plaintiff herself has had her online Amazon and PayPal accounts hacked, unauthorized inquiries appeared on her credit report, and she has experienced a significant increase in spam phone calls, spam test messages as well as spam emails some related to solicitations for medical equipment.

208. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Chambers otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

209. Knowing that thieves stole her child's Private Information, potentially including their PHI and other immutable information, and knowing that her child's Private Information may be available for sale on the dark web, has caused Plaintiff Chambers emotional distress. She is now very concerned about identity theft in general, and what could happen to her child in the future because of the Data Breach.

210. Plaintiff has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

211. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned that her son's Social Security number, which was part of her son's student records at the time of the breach, may have been breached as well.

212. On information and belief, Plaintiff believes that her Private Information including her name, address, phone number and email may have been breached as well because it is part of her child's school records. The likelihood that Plaintiff's

Private Information was part of the Data Breach is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne Murphy, the Data Visualization Designer at Douglas County School District in Colorado.[121]

213. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

214. Plaintiff **Janene Vitro** is a resident of California. Plaintiff is filing these claims as a real party in interest for herself and her son pursuant to Federal Rule of Civil Procedure 17(a)(1)(C). Ms. Vitro's son received a notice letter from Illuminate dated July 29, 2022, stating that his Private Information was compromised by the Data Breach. This letter was sent to her son who is not a minor. Ms. Vitro's son is living with a disability, and she is his legal guardian and legal representative. Her son attended school in the Apple Valley Unified School District in California.

215. In the letter, Defendant stated that it is "now notifying you of this incident because our investigation has determined that your information was contained in the affected databases." The letter went on to disclose that "[t]he affected databases may have contained the following: your name, academic and behavior information, enrollment information, accommodation information, special education information, medical information, and/or student demographic information."

216. As a result of learning of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, researching and signing up for credit monitoring offered by Defendant, calling all three credit agencies to put a credit freeze on her son's credit, sending the credit agencies her power of attorney for the credit freezes, contacting the social security office and her son's bank to inform them of the breach

[121] See ¶ 44 above.

and monitoring her son's financial accounts for fraudulent activity. To date, Plaintiff has spent at least ten hours performing these activities as a result of the Data Breach.

217. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach.

218. In addition, since the breach, Plaintiff's son has experienced an increase in spam phone calls and spam text messages on the number that he had provided to the school. Plaintiff herself has had her online information hacked where the hacker was able to charge her debit card on a fake website.

219. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Vitro otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

220. Knowing that thieves stole her son's Private Information, potentially including his PHI and other immutable information, and knowing that her son's Private Information may be available for sale on the dark web, has caused Plaintiff Vitro emotional distress. She is now very concerned about identity theft in general, and what could happen to her son in the future because of the Data Breach.

221. Plaintiff has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

222. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned that her son's Social Security number, which was part of his student records at the time of the breach, may have been breached as well.

223. On information and belief, Plaintiff believes that her Private Information including her name, address, phone number and email may have been breached as well because it is part of her son's school records. The likelihood that Plaintiff's Private Information was part of the Data Breach is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne Murphy, the Data Visualization Designer at Douglas County School District in Colorado.[122]

224. Plaintiff is experiencing a tremendous amount of anxiety and fear as a direct result of the breach since her son lives with a disability and is extremely vulnerable to fraud and identity theft.

225. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

226. Plaintiff **Lorraine Deniz** is a resident of California. Plaintiff is filing these claims as a real party in interest for herself and her minor children pursuant to Federal Rule of Civil Procedure 17(a)(1)(C). Ms. Deniz received two notice letters from Illuminate dated July 15, 2022, stating that both of her children's Private Information was compromised by the Data Breach. Ms. Deniz' children are minors who attend school in the Fairfield-Suisun Unified School District in California.

227. In the letters, Defendant stated that it "is now notifying you of this incident because our investigation has determined that your minor's information was contained in the affected databases." The letter went on to disclose that "[t]he affected databases may have contained the following: your minor's name, academic and behavior information, enrollment information, accommodation information, special education information, medical information, and/or student demographic information."

[122] See ¶ 44 above.

228. As a result of learning of the Data Breach, To date, Plaintiff spent at least twelve hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, researching and signing up for credit monitoring offered by Defendant, obtaining credit freezes on her children's credit which required her to take time off from work and monitoring her children's information.

229. Plaintiff suffered actual injury in the form of damages to and diminution of the value of Private Information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of education, which was compromised in and as a result of the Data Breach.

230. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Deniz otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

231. Knowing that thieves stole her children's Private Information, potentially including their PHI and other immutable information, and knowing that her children's Private Information may be available for sale on the dark web, has caused Plaintiff Deniz emotional distress. She is now very concerned about identity theft in general, and what could happen to her children in the future because of the Data Breach.

232. Plaintiff has suffered imminent and impending injury arising from the disclosure of their Private Information and for the substantially increased risk of fraud, identity theft, and misuse resulting from Private Information being placed in the hands of unauthorized third parties and criminals.

233. In addition, although Illuminate states in the Data Breach notices that Social Security numbers were not impacted by the Data Breach, Plaintiff is concerned

that her children's Social Security numbers, which were part of their student records, may have been breached as well.

234. Plaintiff has experienced a significant increase in spam phone calls and spam text messages since the Data Breach.

235. On information and belief, Plaintiff believes that her Private Information including her name, address, phone number and email may have been breached as well because it is part of her children's school records. The likelihood that Plaintiff's Private Information was part of the Data Breach is confirmed by the April 13, 2022, email from Adam Smith, Director of Customer Support at Illuminate to Joanne Murphy, the Data Visualization Designer at Douglas County School District in Colorado.[123]

236. Plaintiff has a continued interest in ensuring that Private Information, which remains backed up in Defendant's possession, is protected and safeguarded from further and future breaches.

## CHOICE OF LAW

237. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of Plaintiffs and members of the Nationwide Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

238. The corporate headquarters of Illuminate is located in Irvine, California. California is the "nerve center" of their business activities – the place where their officers direct, control, and coordinate the companies' activities, including their data security functions and policy, financial, and legal decisions.

[123] See ¶ 44 above.

239. Illuminate's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in California.

240. Illuminate's breaches of duty to Plaintiffs and Nationwide Class members emanated from California.

241. Application of California law to the Nationwide Class with respect to Plaintiffs' and Class Members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

242. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Nationwide Class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law and Confidentiality of Medical Information Act may be applied to non-resident plaintiffs as against Illuminate.

## CLASS ACTION ALLEGATIONS

243. Plaintiffs bring this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all others similarly situated.

244. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **Nationwide Class:**
> **All persons in the United States whose Private Information was exposed to unauthorized third parties as a result of the compromise of Illuminate Education, Inc. that occurred between December 2021 and January 2022.**

245. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following state Sub-Classes:

> **Colorado Sub-Class:**
> **All residents of Colorado whose Private Information was exposed to unauthorized third parties as a result**

**of the compromise of Illuminate Education, Inc. that occurred between December 2021 and January 2022.**

**California Sub-Class**:
**All residents of California whose Private Information was exposed to unauthorized third parties as a result of the compromise of Illuminate Education, Inc. that occurred between December 2021 and January 2022.**

**New York Sub-Class:**
**All residents of New York whose Private Information was exposed to unauthorized third parties as a result of the compromise of Illuminate Education, Inc. that occurred between December 2021 and January 2022.**

246. Plaintiffs reserve the right to modify, change, or expand the Class definitions, including proposing additional subclasses, based on discovery and further investigation.

247. Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiffs and Defendant; and (4) legal representatives, successors, or assigns of any such excluded persons.

248. The Classes meet all of the criteria required by Federal Rule of Civil Procedure 23(a).

249. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, it appears that the membership of the Classes are in the tens of thousands. The identities of Class members are also ascertainable through Defendant's records.

250. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions

affecting only individual members of the Class. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

c. Whether and when Defendant actually learned of the Data Breach;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Defendant was negligent or negligent *per se*;

h. Whether Plaintiffs and Class Members are entitled to relief from Defendant as a result of Defendant's misconduct, and if so, in what amounts; and

i. Whether Class Members are entitled to injunctive and/or declaratory relief to address the imminent and ongoing harm faced as a result of the Data Breach.

251. **Typicality:** Plaintiffs' claims are typical of the claims of the Classes they seek to represent, in that the named Plaintiffs and all members of the proposed Classes have suffered similar injuries as a result of the same misconduct alleged herein. Plaintiffs have no interests adverse to the interests of the other members of the Classes.

252. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Classes and have retained attorneys well experienced in class actions and complex litigation as their counsel, including cases alleging breach of privacy and negligence claims arising from corporate misconduct.

253. The Classes also satisfy the criteria for certification under Federal Rule of Civil Procedure 23(b) and 23(c). Among other things, Plaintiffs aver that the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendant has acted or refused to act on grounds that apply generally to the proposed Classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Classes as a whole; that questions of law or fact common to the Classes predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiffs also aver that certification of one or more subclasses or issues may be appropriate for certification under Federal Rule of Civil Procedure 23(c). Plaintiffs further state that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Classes will not be difficult.

254. Plaintiffs and other members of the Classes have suffered damages as a result of Defendant's unlawful and wrongful conduct. Absent a class action, Defendant's unlawful and improper conduct shall, in large measure, not go remedied. Absent a class action, the members of the Classes will not be able to effectively litigate these claims and will suffer further losses.

## CLAIMS FOR RELIEF

### COUNT I
### Negligence

255. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

256. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

257. Illuminate negligently sold its services and products as well protected, claiming that "[w]e take security measures—physical, electronic, and procedural—to help defend against the unauthorized access and disclosure of your information" despite leaving Plaintiffs' and the Classes' Private Information exposed to unauthorized access.

258. Defendant was entrusted with, stored, and otherwise had access to the Private Information of Plaintiffs and Class Members.

259. Defendant knew, or should have known, of the risks inherent to storing the Private Information of Plaintiffs and Class Members, and to not ensuring that its products and services were secure. These risks were reasonably foreseeable to Defendant.

260. Defendant owed duties of care to Plaintiffs and Class Members whose Private Information had been entrusted to them.

261. Further, after discovering that cybercriminals had infiltrated its systems and networks, Illuminate failed to timely notify the schools districts and former and current students or perform a proper forensic analysis of what data had been exposed, consequently, causing notice to Plaintiffs, Class, and Subclass Members to be untimely and insufficient to identify what Private Information had been exposed.

262. Illuminate had additional duties to safeguard Plaintiffs, Class and Subclass Members' data through the following statutes and regulations:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Illuminate had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs, Class and Subclass Members' Private Information.

b. Pursuant to HIPAA, 42 U.S.C. § 1320d, Illuminate had a duty to securely store and maintain the Plaintiffs, Class and Subclass Members' PHI.

c. Pursuant to the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505, Illuminate had a "mandate[d]" duty "get parental consent up front before collecting personal information from children under 13" and to "provide parents with the right to review and delete their children's information." Furthermore, under Section 312.10 of COPPA, Illuminate could only "retain children's personal information 'for only as long as is reasonably necessary to fulfill the purpose for which the information was collected[,]'" and thereafter had a duty to "delete [children's personal information] using reasonable measures to ensure it's been securely destroyed" even absent a parent's request for the deletion of a child's personal information.[124]

d. Pursuant to the New York Education Law § 2-d, Illuminate had a duty to securely store and maintain the Plaintiffs, Class and Subclass Members' Private Information. The New York Education Law § 2d requires that "Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data shall: except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party: uses encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States

[124] *See* FTC, *Under COPPA, data deletion isn't just a good idea. It's the law*. (May 31, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law (last visited October 31, 2022).

department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5." New York Education Law § 2-d, 5. f. (3) and (5).

263. Illuminate's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Illuminate is bound by industry standards to protect confidential Private Information.

264. Illuminate breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs, Class and Subclass Members' data. The specific negligent acts and omissions committed by Illuminate include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs, Class and Subclass Members; Private Information;

b. Failing to maintain the PHI and PI of Plaintiffs and the Class and Subclass in encrypted form;

c. Failing to adequately monitor the security of its networks and systems;

d. Allowing unauthorized access to and exfiltration of Plaintiffs, Class, Subclass Members' Private Information;

e. Failing to timely detect that Plaintiffs, Class and Subclass Members' Private Information had been compromised;

f. Failing to provide timely notice that Plaintiffs, Class and Subclass Members' Private Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to provide adequate notice of what Private Information had been compromised so that Plaintiffs, Class and Subclass Members at risk could take timely and appropriate steps to mitigate the potential for identify theft and other damages.

265. It was foreseeable to Illuminate that its failure to use reasonable measures to protect Plaintiffs, Class and Subclasses Members' Private Information, including when it was warned its systems and networks were vulnerable to cyberattack, would result in injury to Plaintiffs, Class and Subclass members. Further, the breach of security was reasonably foreseeable given the known high frequency of [redacted].

266. It was additionally foreseeable to Illuminate that failure to timely and adequately provide notice of the Data Breach would result in Plaintiffs, Class and Subclass Members not being afforded the ability to timely safeguard their identities.

267. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security in connection with marketing, sale, and use of its services and products. Defendant had a duty to safeguard Plaintiffs' and Class Members' Private Information and to ensure that their systems and products adequately protected Private Information.

268. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

269. Defendant acted with wanton disregard for the security of Plaintiffs' and Class Members' Private Information.

270. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

271. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

272. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members face an increased risk of future harm.

273. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

274. Plaintiffs are also entitled to injunctive relief requiring Illuminate to, e.g., (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class members, and any other relief this Court deems just and proper.

275. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members and are entitled to damages in an amount to be proven at trial.

## COUNT II
## Negligence Per Se

276. Plaintiffs reallege each and every allegation contained above, and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

277. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

278. Pursuant to the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Defendant had a duty to provide adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

279. Pursuant to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g, Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

280. Pursuant to HIPAA, 42 U.S.C. § 1320d, Illuminate had a duty to securely store and maintain the Plaintiffs, Class and Subclass Members' PHI.

281. Pursuant to the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq.*, Defendant had a duty to implement reasonable and adequate safeguards and security practices to protect Plaintiffs' and Class Members' Private Information.

282. Pursuant to the Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. § 6501-6505, Defendant had a duty to provide adequate data security practices to safeguard Plaintiffs' and Class Members' Private Information.

283. Pursuant to the COPPA, Illuminate had a duty to: (i) get parental consent before collecting personal information from children under 13; (ii) provide parents with the right to review and delete their children's information; and (iii) could only retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected, and thereafter had a duty to delete any and all children's personal information using reasonable measures to ensure it's been securely destroyed, even absent a parent's request for the deletion of a child's personal information.

284. Pursuant to other state and federal laws requiring the confidentiality of Private Information, including, but not limited to, the FTC Act, FERPA, and COPPA, among other laws, Defendant had a duty to implement reasonably safeguards to protect Plaintiffs' and Class Members' Private Information.

285. Defendant breached its duties to Plaintiffs and Class Members under the

FTC Act, FERPA, and COPPA, among other laws, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiffs' and Class Members' Private Information.

286. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

287. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

288. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that its breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

289. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members face an increased risk of future harm.

290. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT III
## Invasion of Privacy

291. Plaintiffs reallege each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

292. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado and California Subclasses.

293. Plaintiffs and Class Members had a reasonable and legitimate expectation of privacy in the Private Information that Defendant disclosed without authorization.

294. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

295. Defendant failed to protect and release to unknown and unauthorized third parties the Private Information of Plaintiffs and Class Members.

296. By failing to keep Plaintiffs' and Class Members' Private Information safe and disclosing Private Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Member's privacy by, among others, (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) improperly using their Private Information properly obtained for a specific purpose for another purpose, or disclosing it to a third party; (iii) failing to adequately secure their Private Information from disclosure to unauthorized persons; and (iv) enabling the disclosure of Plaintiffs' and Class Members' Private Information without consent.

297. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider their actions highly offensive.

298. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted, and caused damages to Plaintiffs and Class Members.

299. In failing to protect Plaintiffs' and Class Members' Private Information, and in disclosing Plaintiffs' and Class Members' Private Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

300. Plaintiffs seek injunctive relief on behalf of the Classes, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment

for monetary damages will not end the invasion of privacy for Plaintiffs and the Classes.

**COUNT IV**
**Breach of Confidence**

301. Plaintiffs reallege each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

302. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

303. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Private Information that Plaintiffs and Class Members provided to Defendant.

304. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

305. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

306. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

307. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to unauthorized third parties or to the public.

308. Due to Defendant's failure to prevent and avoid the Data Breach from

occurring, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

309. As a proximate result of such unauthorized disclosures, Plaintiffs and Class Members suffered damages.

310. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, access, and used by unauthorized third parties.

311. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known that its methods of accepting, storing, transmitting, and using Plaintiffs' and Class Members' Private Information was inadequate.

312. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

313. As a direct proximate result of such unauthorized disclosures, Plaintiffs

and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**COUNT V**
**Breach of Contract**

314. Plaintiffs reallege each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

315. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

316. Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

317. Plaintiffs and the Class Members are parties to contracts with Illuminate. Under the circumstances, recognition of a right to performance by Plaintiffs and the Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiffs and the Class Members the benefit of the performance promised in the contracts. Additionally, and/or in the alternative, Plaintiffs and Class Members were intended third-party beneficiaries of the contracts between Illuminate and their respective school districts/governing bodies, and therefore are able to enforce their rights under the contracts. Illuminate intended to benefit Plaintiffs and the Class when it came into possession of the Private Information through contracts that it entered into with the students' school districts, pursuant to which it stored the students' Private Information.

318. Defendant breached these agreements, which directly and/or proximately caused Plaintiffs and the Class Members to suffer substantial damages.

319. Accordingly, Plaintiffs and Class Members are entitled to damages,

restitution, disgorgement of profits and other relief in an amount to be proven at trial.

**COUNT VI**
**Invasion of Privacy**

320. Plaintiffs reallege each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

321. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

322. California established the right to privacy in Article 1, Section 1 of the California Constitution.

323. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977).

324. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

325. Defendant owed a duty to current and former students, including Plaintiffs and Class Members, to keep their Private Information confidential.

326. The unauthorized release of Private Information, especially the type related to personal health information, is highly offensive to a reasonable person.

327. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the

intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

328. The Data Breach constitutes an intentional interference with Plaintiffs" and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

329. Defendant acted with a knowing state of mind when they permitted the Data Breach because they knew its information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiffs and Class Members.

330. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

331. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' Private Information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiffs and Class Members to suffer damages.

332. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

333. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

**COUNT VII**
**Violation of the California Consumer Privacy Act,**
**Cal. Civil Code §§ 1798.100, *et seq*.**

334. Plaintiffs Chambers, Vitro and Deniz ("California Plaintiffs") reallege each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

335. California Plaintiffs brings this claim on behalf of the Class.

336. At all times during California Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of California Plaintiffs' and Class Members' Private Information that California Plaintiffs and Class Members provided to Defendant.

337. Defendant is a business under California Civil Code 1798.140(c) because it collects PII and PHI. On information and belief, Defendant, alone, or jointly with others, such as educators using Defendant's platforms, use the collected PII and PHI to determine what academic or behavioral interventions or next steps are necessary. It is also plausible that Defendant processes the collected PII and PHI to further develop its many platforms.

338. Defendant's relationship with California Plaintiffs and Class Members was governed by terms and expectations that California Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

339. California Plaintiffs and Class Members provided their Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

340. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, California Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

341. Through the above-detailed conduct, Defendant violated California Civil Code section 1798.150 by failing to prevent California Plaintiffs' and Class Members' nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

342. As a proximate result of such unauthorized disclosures, California Plaintiffs' and Class Members' Private Information, including, among others, names, dates of birth, academic information, special education status, financial status, and contact information, was subjected to unauthorized access and exfiltration, theft, and disclosure.

343. California Plaintiffs seek injunctive relief on behalf of the Classes as well as other equitable relief. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to California Plaintiffs and Class Members. California Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for California Plaintiffs and the Classes.

344. In accordance with Civil Code section 1798.150(b), California Plaintiffs will serve Defendant with notice of violation of Civil Code section 1798.150(a) and a demand for relief. If Defendant fails to properly respond to California Plaintiffs notice letter or agree to timely and adequately rectify the violations detailed above, Plaintiffs will also seek actual, punitive, and statutory damages, as well as restitution, attorneys' fees and costs, and any other relief the Court deems proper.

## COUNT VIII
## Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

345. Plaintiffs Chambers, Vitro and Deniz ("California Plaintiffs") reallege each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

346. California Plaintiffs bring this claim on behalf of the Class.

347. California Plaintiffs, the members of the Class, and Defendant are a "person" or "persons," within the meaning of Section 17201 of the California Unfair Competition Law ("UCL").

348. Defendant has engaged in unfair competition within the meaning of California Business & Professions Code section 17200, *et seq.*, because Defendant's conduct, as described herein, violated the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.* Further, Defendant breached its duties pursuant to the FTC Act, 15 U.S.C. § 45, FERPA, HIPAA, CCPA, and COPPA to implement reasonable safeguards to protect California Plaintiffs' and Class Member's Private Information. Thus, Defendant violated the UCL's unlawful, unfair, and fraudulent prongs.

349. Defendant's conduct, as described herein, violated the UCL's unlawful prong because it violates the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, the FTC Act, 15 U.S.C. § 45, FERPA, HIPAA, CCPA, and COPPA.

350. Defendant's conduct, as described herein, violated the UCL's unfair prong because Defendant promised adequate data privacy and security practices and procedures when such practices were deficient. Additionally, these unfair acts and practices were immoral unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws named herein. Defendant likewise engaged in unfair acts and practices by failing to disclose the Data Breach in a timely and accurate manner.

351. Plaintiffs and the Class may proceed under the balancing or tethering test because on balance, the gravity of Defendant's violations of children's privacy rights vastly outweighs the utility of its conduct and because Plaintiffs have identified

a number of important public policy considerations and statutes that Defendant has violated.

352. Defendant's conduct, as described herein, violated the UCL's fraudulent prong by representing that it would maintain adequate data privacy and security practices and procedures to safeguard PII and PHI, representing and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class's PII and PHI, and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's PII and PHI.

353. California Plaintiffs have standing to pursue this claim because they have been injured by virtue of the wrongful conduct alleged herein.

354. The Unfair Competition Law is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or common law remedies, such as those alleged in the other Counts of this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

355. As a direct and proximate cause of Defendant's conduct, which constitutes unlawful business practices as alleged herein, California Plaintiffs and Class Members have been damaged and suffered ascertainable losses due to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect California Plaintiffs' and Class Members' Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect,

contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of California Plaintiffs and Class Members.

356. California Plaintiffs and Class Members are thereby entitled to recover restitution and equitable relief, including disgorgement or ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, filing fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

**COUNT IX**
**Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.***

357. Plaintiffs Chambers, Vitro and Deniz ("California Plaintiffs") reallege each and every allegation contained above and incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

358. California Plaintiffs bring this claim on behalf of the Class.

359. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

360. Illuminate is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about California Plaintiffs and Class Members.

361. Businesses that own or license computerized data that includes personal information, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible

and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." *Id.*

362. Illuminate is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

363. California Plaintiffs and Class Members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

364. Because Illuminate reasonably believed that California Plaintiffs and Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Illuminate had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

365. By failing to disclose the Data Breach in a timely and accurate manner, Illuminate violated Cal. Civ. Code § 1798.82.

366. As a direct and proximate result of Illuminate's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, California Plaintiffs' and Class Members suffered damages, as described above.

367. California Plaintiffs and Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

## COUNT X
## Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*

368. Plaintiffs Chambers, Vitro and Deniz ("California Plaintiffs") reallege each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

369. California Plaintiffs brings this claim on behalf of the Class.

370. The California Confidentiality of Medical Information Act ("CMIA") prohibits, among other things, unauthorized disclosure of private medical information. Cal. Civ. Code §§ 56, et seq.

371. California Plaintiffs provided their PHI to the schools they attended which is a "health care practitioner" and is a "provider of health care" as defined by Cal. Civ. Code § 56.05(j).

372. California Plaintiffs are "patients" as defined by Cal. Civ. Code § 56.05(k).

373. Illuminate is a "provider of health care" subject to the CMIA because it is a "business that offers software or hardware to consumers, . . . that is designed to maintain medical information" in order to make the information available to an individual to which California Plaintiffs provided their PHI. Cal. Civ. Code § 56.06.

374. Illuminate stored in electronic form on its computer system California Plaintiffs' "medical information" as defined by Cal. Civ. Code § 56.05(j).

375. Illuminate's systems were designed, in part, to make medical information available to schools by providing cloud-based computing solutions through which the schools could store, access, and manage current and former students' medical information that are part of their school records.

376. California Plaintiffs did not provide Illuminate authorization nor was Illuminate otherwise authorized to disclose California Plaintiffs' medical information to an unauthorized third-party.

377. As described throughout this Complaint, Illuminate negligently maintained, disclosed and released California Plaintiffs' and the Class Members PHI inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

378. As a direct and proximate result of Illuminate's negligence, it disclosed and released California Plaintiffs' and Class Members' PHI to an unauthorized third-party.

379. Illuminate's unauthorized disclosure of former and current students' medical information that are part of their school records has caused injury to the California Plaintiffs and the Class Members.

380. Upon information and belief, California Plaintiffs' PHI was viewed by an unauthorized third party.

381. Accordingly, California Plaintiffs', individually and on behalf of the California Subclass, seek to recover actual, nominal (including $1000 nominal damages per disclosure under § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

## COUNT XI
## Colorado Security Breach Notification Act, Colo. Rev. Stat. §§ 6-1-716, *et seq.*

382. Plaintiffs Cranor and Weiland ("Colorado Plaintiffs"), reallege each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

383. Colorado Plaintiffs bring this claim on behalf of the Colorado Subclass.

384. Illuminate is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

385. Illuminate is required to accurately notify Colorado Plaintiffs and Colorado Subclass Members if it becomes aware of a breach of its data security program in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

386. Because Illuminate was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

387. By failing to disclose the Data Breach in a timely and accurate manner, Illuminate violated Colo. Rev. Stat. § 6-1-716(2).

388. As a direct and proximate result of Illuminate's violations of Colo. Rev.

Stat. § 6-1-716(2), Colorado Plaintiffs and Colorado Subclass Members suffered damages, as described above.

389. Colorado Plaintiffs and Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

## COUNT XII
## Colorado Consumer Protection Act, Colo. Rev. Stat. §§ 6-1-101, *et seq.*

390. Plaintiffs Cranor and Weiland ("Colorado Plaintiffs"), reallege each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

391. Colorado Plaintiffs bring this claim on behalf of the Colorado Subclass.

392. Illuminate is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6). Illuminate engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

393. Colorado Plaintiffs and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Illuminate or successors in interest to actual consumers.

394. Illuminate engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including, but not limited to:

395. Knowingly making a false representation as to the characteristics of products and services;

396. Representing that services are of a particular standard, quality, or grade, though Illuminate knew or should have known that there were or another;

397. Advertising services with intent not to sell them as advertised; and

398. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

399. Failing to implement and maintain reasonable security and privacy measures to protect Colorado Plaintiffs and Colorado Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

400. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach.

401. Failing to comply with common law and statutory duties pertaining to the security and privacy of Colorado Plaintiffs and Colorado Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and FERPA, among other laws, which was a direct and proximate cause of the Data Breach; and

402. Misrepresenting that it would protect the privacy and confidentiality of Colorado Plaintiffs' and Colorado Subclass members' Private Information, including by implementing and maintaining reasonable security measures.

403. Illuminate also violated Colo. Rev. Stat. § 6-1-105(1) by committing the acts described throughout.

404. Illuminate's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Illuminate's data security and ability to protect the confidentiality of consumers' Private Information.

405. Illuminate's representations and omissions were material because they were likely to deceive reasonable consumers, including Colorado Plaintiffs and the Colorado Subclass Members, that their Private Information was not exposed and misled Colorado Plaintiffs' and the Colorado Subclass Members into believing they did not need to take actions to secure their identities.

406. Illuminate intended to mislead Colorado Plaintiffs and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

407. Had Illuminate disclosed to Colorado Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Illuminate would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Illuminate was trusted with sensitive and valuable Private Information regarding an untold number

of students, including Colorado Plaintiffs, the Class, and the Colorado Subclass. Illuminate accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Illuminate held itself out as maintaining a secure platform for Private Information, Colorado Plaintiffs, the Class, and the Colorado Subclass Members acted reasonably in relying on Illuminate's misrepresentations and omissions, the truth of which they could not have discovered.

408. Illuminate acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Colorado Plaintiffs and Subclass Members' rights.

409. As a direct and proximate result of Illuminate's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

410. Illuminate's deceptive trade practices significantly impact the public, as numerous Colorado school districts were affected, and a yet untold number of students' Private Information was disclosed.

411. Colorado Plaintiffs and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Illuminate's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

## COUNT XIII
## New York General Business Law § 349

412. Plaintiff Kisil, realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

413. Plaintiff brings this claim on behalf of the New York Subclass.

414. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

(a) Defendant misrepresented material facts to Plaintiff and Class Members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and New York Class Members' Private Information and other data from unauthorized disclosure, release, data breaches, and theft;

(b) Defendant misrepresented material facts to Plaintiff and New York Class Members by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff and New York Class Members' Private Information and other data;

(c) Defendant omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Plaintiff and New York Subclass Members' Private Information and other data;

(d) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff and New York Subclass Members' Private Information and other data, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

(e) Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law §§ 899-aa(2) and 899-bb (SHIELD Act).

415. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers

(including Plaintiff and New York Subclass Members) regarding the security of its network and aggregation of Private Information and other data.

416. Defendant omitted material facts including that it possessed and maintained Plaintiffs and the New York Subclass' PHI and PI, [redacted]

417. The misrepresentations made to consumers (including Plaintiff and New York Subclass Members) were material misrepresentations (e.g., as to Defendant's adequate protection of Private Information and other data), and consumers (including Plaintiff and New York Subclass Members).

418. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and New York Subclass Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability of their Private Information and other data.

419. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff and New York Subclass Members' Private Information and other data were disclosed to third parties without authorization, causing and will continue to cause Plaintiff and New York Subclass Members damages.

420. As a direct and proximate result of Defendant's violation of NY GBL §349, Plaintiff and New York Subclass Members have suffered, and continue to suffer, injuries, damages arising from identify theft; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with

credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

421. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, injunctive relief, and reasonable attorneys' fees and costs.

422. The above constitutes violation of NY GBL §349.

423. An actual controversy has arisen and now exists between Plaintiff and the putative Classes on the one hand, and Defendant on the other, concerning Defendant's failure to protect Plaintiff's and New York Subclass Members' Private Information in accordance with applicable state and federal regulations and the agreements between the parties. Plaintiff and the New York Subclass Members contend that Defendant failed to maintain adequate and reasonable privacy practices to protect their Private Information while on the other hand, Defendant contends they have complied with applicable state and federal regulations and its agreements with Plaintiff and New York Subclass Members to protect their Private Information.

424. Accordingly, Plaintiff and New York Subclass Members are entitled to and seek a judicial determination of whether Defendant has performed, and are performing, their statutory and contractual privacy practices and obligations necessary to protect and safeguard Plaintiff's and New York Subclass Members' Private Information from further unauthorized, access, use, and disclosure, or insecure disposal.

425. A judicial determination of the rights and responsibilities of the parties over Defendant's privacy practices is necessary and appropriate at this time so that: (1) that the rights of the Plaintiff and the New York Subclass Members may be determined with certainty for purposes of resolving this action; and (2) so that the Parties will have an understanding of Defendant's obligations in the future given its continuing legal obligations and ongoing relationships with Plaintiffs and New York Subclass Members.

**COUNT XIV**
**Declaratory Relief**
**28 U.S.C. § 2201**

426. Plaintiffs reallege each and every allegation contained above and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

427. Plaintiffs bring this claim on behalf of the Class, or in the alternative, the Colorado, California and New York Subclasses.

428. An actual controversy has arisen and now exists between Plaintiffs and the putative Classes on the one hand, and Defendant on the other, concerning Defendant's failure to protect Plaintiffs' and Class Members' Private Information in accordance with applicable state and federal regulations and the agreements between the parties. Plaintiffs and the Class Members contend that Defendant failed to maintain adequate and reasonable privacy practices to protect their Private Information while on the other hand, Defendant contends they have complied with applicable state and federal regulations and its agreements with Plaintiffs and Class Members to protect their Private Information.

429. Accordingly, Plaintiffs and Class Members are entitled to seek a judicial determination of whether Defendant has performed, and are performing, their statutory and contractual privacy practices and obligations necessary to protect and safeguard Plaintiffs' and Class Members' Private Information from further unauthorized, access, use, and disclosure, or insecure disposal.

430. A judicial determination of the rights and responsibilities of the parties over Defendant's privacy practices is necessary and appropriate at this time so that: (1) that the rights of the Plaintiffs and the Classes may be determined with certainty for purposes of resolving this action; and (2) so that the Parties will have an understanding of Defendant's obligations in the future given its continuing legal obligations and ongoing relationships with Plaintiffs and Class Members.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of the Classes, prays for relief as follows:

A. For an Order certifying this case as a class action pursuant to Federal Rule of Civil Procedure 23 against Defendant, appointing Plaintiffs as Class Representative of the Class and/or Subclasses;

B. Awarding monetary, punitive and actual damages and/or restitution, as appropriate;

C. Awarding declaratory and injunctive relief as permitted by law or equity to assure that the Classes have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Prejudgment interest to the extent allowed by the law;

E. Awarding all costs, experts' fees and attorneys' fees, expenses and costs of prosecuting this action; and

F. Such other and further relief as the Court may deem just and proper.

## JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully submitted,

DATED: June 5, 2023

**KAPLAN FOX & KILSHEIMER LLP**

By: /s/ *Laurence D. King*
Laurence D. King

Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
Email: *lking@kaplanfox.com*
*mgeorge@kaplanfox.com*
*breed@kaplanfox.com*

**KAPLAN FOX & KILSHEIMER LLP**
Joel B. Strauss (admitted *pro hac vice*)
800 Third Avenue, 38th Floor
New York, NY 10022
Telephone: 212-687-1980
Facsimile: 212-687-7714
Email: *jstrauss@kaplanfox.com*

**KAPLAN FOX & KILSHEIMER LLP**
Justin B. Farar (SBN 211556)
12400 Wilshire Boulevard, Suite 460
Los Angeles, CA 90025
Telephone: 310-614-7260
Email: *jfarar@kaplanfox.com*

**KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.**

By: /s/ *Melissa R. Emert*
Melissa R. Emert

Melissa R. Emert (admitted *pro hac vice*)
Gary S. Graifman (admitted *pro hac vice*)
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Email: *memert@kgglaw.com*
*ggraifman@kgglaw.com*

*Interim Co-Lead Class Counsel*

**HELD AND HINES LLP**
Marc J. Held (admitted *pro hac vice*)
Philip M. Hines (admitted *pro hac vice*)
2044 Ralph Avenue
Brooklyn, NJ 11234
Telephone: 718-531-9700
Email: *mheld@heldhines.com*
*phines@heldhines.com*

**SHEEHAN AND ASSOCIATES, P.C.**
Spencer Sheehan (admitted *pro hac vice*)
60 Cuttermill Road, Suite 409
Great Neck, NY 11021
Telephone: 516-268-7080
Email: *spencer@spencersheehan.com*

**SHEEHAN AND ASSOCIATES, P.C.**
Theodore Hillebrand
65-24 78th Street
Middle Village, NY 11379
Telephone: 929-246-0747
Email: *thillebrand@spencersheehan.com*

*Plaintiffs' Executive Committee*

*Attorneys for Plaintiffs and the Proposed Class*